Penerapan Kurva Eliptik Atas Zp Pada Skema Tanda Tangan Elgamal

Oleh :
Puguh Wahyu Prasetyo
S2 Matematika, Universitas Gadjah Mada, Yogyakarta
Email : puguhwp@gmail.com

Muhamad Zaki Riyanto
S2 Matematika, Universitas Gadjah Mada, Yogyakarta
Email : zaki@mail.ugm.ac.id

Abstrak

Kurva eliptik yang didefinisikan atas Z_p mempunyai peranan penting dalam perkembangan sistem kriptografi maupun pada skema tanda tangan. Tingkat keamanan kurva eliptik atas Z_p terletak pada tingkat kesulitan *Elliptic Curve Discrete Logarithm Problem* (ECDLP), karena tidak ada algoritma yang efisien untuk menyelesaikan ECDLP. Hal ini berbeda dengan permasalahan matematis logaritma diskrit (*Discrete Logarithm Problem*, DLP) dan pemfaktoran bilangan bulat (*Integer Factorization Problem*, IFP). Ada tiga protokol ECDLP yang diketahui saat ini yaitu *Elliptic Curve Digital Signature Algorithm (ECDSA)*, *Elliptic Curve Diffie Hellman (ECDH*), dan *Elliptic Curve ElGamal (ECElgamal)*. Pada makalah ini membahas tentang penerapan kurva eliptik yang didefinisikan atas Z_p pada skema tanda tangan ElGamal, yaitu *ECElgamal* yang diterapkan pada skema tanda tangan.

Kata Kunci : *Kurva Eliptik atas Z_p, Elliptic Curve Discrete Logarithm Problem* (ECDLP), *skema tanda tangan, skema tanda tangan ElGamal.*

1. Pendahuluan

Saat ini teknologi informasi berkembang sangat pesat, komunikasi dari satu pihak kepihak yang lain dapat dilakukan melalui media internet, sehingga waktu yang digunakan untuk berkomunikasi relatif sangat singkat, akan tetapi seiring berkembangnya teknologi pula, muncul pihak-pihak yang tidak resmi berkomunikasi yang sengaja menyadap maupun mengubah pesan yang dikirim pada suatu sesi komunikasi. Sehingga diperlukan suatu ilmu untuk menyelesaikan permasalahan tersebut, maka berkembanglah kriptografi.

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematis sedemikian hingga dapat menyembunyikan suatu informasi atau pesan asli (*plaintext*) menjadi sebuah teks tersembunyi (*chipertext*) dan kemudian diubah menjadi pesan asli kembali. Hal ini menunjukkan bahwa kriptografi berhubungan dengan aspek keamanan informasi seperti aspek kerahasiaan, keabsahan, integritas, dan keaslian. Secara umum, kriptografi terdiri dari proses pembentukan kunci, proses enkripsi, dan proses dekripsi. *Enkripsi* adalah sebuah proses persandian yang melakukan perubahan *plaintext* menjadi sebuah *ciphertext*. Sedangkan proses untuk mengubah *ciphertext* menjadi *plaintext* disebut *dekripsi*. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu. Kebalikan dari kriptografi adalah kriptanalisis, dilakukan oleh pihak penyerang untuk mendapatkan kunci yang dapat digunakan untuk mengetahui *plaintext.* Dalam suatu sesi komunikasi dengan pihak lain, terkadang diperlukan proses pertukaran informasi, sehingga membutuhkan adanya suatu mekanisme untuk menjamin keaslian informasi yang bersangkutan. Salah satu cara yang digunakan untuk mengatasi permasalahan di atas adalah dengan cara menambahkan tanda tangan (*signature*) pada informasi atau dokumen tersebut. Salah satu sistem kriptografi yang cocok untuk skema

tanda tangan adalah sistem kriptografi ElGamal yang didefinisikan atas Grup Eliptik atas Z_p.

2. Grup Eliptik atas Z_p

Kurva Eliptik yang didefinisikan atas Z_p merupakan materi terpenting grup eliptik atas Z_p, karena proses tanda tangan dan verifikasi suatu dokumen yang dibubuhi tanda tangan menggunakan titik-titik pada kurva eliptik atas Z_p yang membentuk grup eliptik atas Z_p, beserta dengan operasi-operasi yang berlaku pada kurva eliptik atas Z_p.

Definisi. (Stinson, 2006 : 258)

Misalkan p adalah sebuah bilangan prima yang lebih besar dari 3. Kurva eliptik atas Z_p didefinisikan oleh :

$$E(Z_p) = \{(x,y) \in Z_p \times Z_p \mid y^2 \equiv x^3 + ax + b \pmod p\} \cup \{\theta\}$$

dengan $a,b \in Z_p$ sedemikian hingga $4a^3 + 27b^2 \not\equiv 0 \pmod p$. Titik θ disebut dengan titik *infinity* atau titik infinitas, dan titik-titik pada kurva eliptik atas Z_p membentuk suatu grup, yaitu grup eliptik atas Z_p.

Operasi – Operasi pada Kurva Eliptik atas Z_p

Diberikan suatu kurva eliptik atas Z_p, yaitu $E(Z_p) : y^2 = x^3 + ax + b \bmod p$ dengan titik *infinity* sebagai elemen identitas terhadap operasi penjumlahan. Berikut dijelaskan beberapa kasus penjumlahan dua titik pada kurva eliptik $E(Z_p)$. Misalkan $P, Q \in E(Z_p)$ dengan $P = (x_1,y_1)$ dan $Q = (x_2,y_2)$, untuk penjumlahan dua titik tersebut terdapat tiga kasus, yaitu :

Kasus I

Apabila $x_1 \neq x_2$. Misalkan terdapat suatu garis L, yang memotong kurva eliptik $E(Z_p)$ dan melalui kedua titik tersebut, yaitu titik P dan Q. Maka persamaan garis L adalah :

$$y = \lambda x + v \qquad (2.1)$$

dengan kemiringan

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad (2.2)$$

dan

$$v = y_1 - \lambda x_1 = y_2 - \lambda x_2 .$$

Untuk mendapatkan titik-titik pada $E(Z_p)$ yang dilalui garis L, substitusi persamaan 3.1 kedalam persamaan kurva eliptik $y^2 = x^3 + ax + b$, sehingga diperoleh :

$$(\lambda x + v)^2 = x^3 + ax + b$$

$$x^3 - \lambda^2 x^2 + (a - 2\lambda v)x + b - v^2 = 0 \qquad (2.3)$$

Jika x_1, x_2, x_3 merupakan solusi dari persamaan $y^2 = x^3 + ax + b$ maka berlaku :

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - (x_1x_2x_3) = 0 \qquad (2.4)$$

Dari persamaan 2.3 dan 2.4 diperoleh

$$x_3 = \lambda^2 - x_1 - x_2 \qquad (2.5)$$

Untuk mencari nilai y_3, harus dihitung kemiringan dari suatu garis yang melalui titik (x_1,y_1) dan $(x_3, -y_3)$, yaitu :

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1} \qquad (2.6)$$

Dari persamaan 3.6 diperoleh

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (2.7)$$

Dari penjabaran diatas dapat disimpulkan bahwa pada kasus I, untuk penjumlahan dua titik P, $Q \in E(Z_p)$ dengan $P = (x_1,y_1)$ dan $Q = (x_2,y_2)$. Jika $x_1 \neq x_2$,maka

$(x_1,y_1) + (x_2,y_2) = (x_3,y_3)$ (2.8)

dengan

$$x_3 = \lambda^2 - x_1 - x_2 \quad (2.9)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (2.10)$$

dan

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad (2.11)$$

Kasus II

Apabila $x_1 = x_2$ dan $y_1 = -y_2$ atau dengan kata lain, untuk penjumlahan dua titik P, $Q \in E(Z_p)$ dengan $P = (x_1,y_1)$ dan $Q = (x_1,-y_1)$, maka

$(x_1, y_1) + (x_1,-y_1) = (x_3, y_3)$

Untuk mencari x_3 dan y_3, maka harus dicari kemiringan garis L, yaitu suatu garis yang memotong kurva eliptik $E(Z_p)$, dan melalui titik $P = (x_1,y_1)$ dan $Q = (x_1,-y_1)$, yaitu :

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = = \frac{y_2 + y_2}{x_2 - x_2} = \infty$$

Kemudian substitusi $\lambda = \infty$ ke persamaan 3.9 dan 3.10, sehingga diperoleh :

$x_3 = \infty$

$y_3 = \infty$

atau

$(x_3,y_3) = \theta$

Dari penjabaran diatas dapat disimpulkan bahwa $(x,y) + (x,-y) = \theta$, $\forall (x, y) \in E(Z_p)$.

Kasus III

Apabila $x_1 = x_2$ dan $y_1 = y_2$ atau dengan kata lain, apabila diberikan suatu titik $P = (x_1,y_1) \in E(Z_p)$, maka penggandaan atas titik P, yaitu $P + P$ adalah :

$(x_1,y_1) + (x_1,y_1) = (x_3,y_3)$

Untuk mencari x_3 dan y_3, maka harus dicari kemiringan garis L, yaitu suatu garis yang memotong kurva eliptik $E(Z_p)$ dan melalui titik $P = (x_1,y_1)$, dengan mencari turunan pertama dari persamaan kurva eliptik : $y^2 = x^3 + ax + b$ terhadap x. Turunan pertama dari persamaan kurva eliptik tersebut adalah :

$$2y\frac{dy}{dx} = 3x^2 + a \quad (2.12)$$

Atau

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y} \quad (2.13)$$

Karena $\lambda = \frac{dy}{dx}$, maka dari persamaan 3.13 diperoleh

$$\lambda = \frac{3x^2 + a}{2y}$$

Substitusi $x = x_1$ dan $y = y_1$, sehingga diperoleh :

$$\lambda = \frac{3x_1^{\,2} + a}{2y_1} \qquad (2.14)$$

Untuk mendapatkan titik-titik pada $E(Z_p)$ yang dilalui garis L, substitusi persamaan 3.1 kedalam persamaan kurva eliptik $y^2 = x^3 + ax + b$, sehingga diperoleh :

$$x^3 - \lambda^2 x^2 + (a - 2\lambda v)x + b - v^2 = 0 \qquad (2.15)$$

Jika x_1, x_2, x_3 merupakan solusi dari persamaan (3.15) maka berlaku :

$$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - (x_1x_2x_3) = 0 \qquad (2.16)$$

Dari persamaan 3.15 dan 3.16 diperoleh

$$x_3 = \lambda^2 - x_1 - x_2 \qquad (2.17)$$

Untuk mencari nilai y_3, harus dihitung kemiringan dari suatu garis yang melalui titik (x_1,y_1) dan $(x_3,-y_3)$, yaitu :

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1} \qquad (2.18)$$

Dari persamaan 3.18 diperoleh

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad (2.19)$$

Dari penjabaran diatas dapat disimpulkan bahwa pada kasus III, untuk penggandaan atas titik $P \in E(Z_p)$ dengan $P = (x_1,y_1)$, maka

$$(x_1,y_1) + (x_1,y_1) = (x_3,y_3) \qquad (2.20)$$

dengan

$$x_3 = \lambda^2 - x_1 - x_2 \qquad (2.21)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \qquad (2.22)$$

dan

$$\lambda = \frac{3x_1^{\,2} + a}{2y_1} \qquad (2.23)$$

Dari penjabaran diatas, maka dapat disimpulkan bahwa operasi-operasi yang berlaku pada kurva Eliptik $E(Z_p)$: $y^2 = x^3 + ax + b$ atas Z_p antara lain :

Kurva Eliptik $E(Z_p)$ mempunyai elemen identitas terhadap operasi penjumlahan, yaitu titik θ, sehingga $P + \theta = \theta + P = P$, untuk semua $P \in E(Z_p)$.

Untuk setiap titik pada kurva Eliptik E(Zp) mempunyai invers terhadap operasi penjumlahan atau secara matematis

$\forall P = (x, y) \in E(Z_p), \exists -P = (x,-y) \in E(Z_p), \ni P + (-P) = \theta$.

Penjumlahan titik.

Misalkan $P = (x_1, y_1) \in E(Z_p), dan\ Q = (x_2, y_2) \in E(Z_p)$, dengan $P \neq \pm Q$, maka $P + Q = (x_3, y_3)$, dengan

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \text{ dan } y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.$$

Penggandaan titik.

Misalkan $P = (x_1, y_1) \in E(Z_p)$, dengan $P \neq -P$. Maka $2P = P+P = (x_3,y_3)$, dengan

$$x_3 = \left(\frac{3x_1^{\,2} + a}{2y_1}\right)^2 - 2x_1 \text{ dan } y3 = \left(\frac{3x_1^{\,2} + a}{2y_1}\right)(x_1 - x_3) - y_1.$$

3. Skema Tanda Tangan Elgamal pada Grup Eliptik atas Z_p

Dalam suatu sesi komunikasi, yaitu pada pengiriman pesan, tidak menutup kemungkinan pesan tersebut sengaja diubah dan dimodifikasi oleh pihak lain yang tidak terlibat komunikasi secara legal. Oleh sebab itu perlu dilakukan proses otentifikasi, yaitu dengan menunjukkan bahwa suatu pesan tersebut memang benar dari pihak pengirim pesan resmi. Salah satu cara untuk melakukan proses otentifikasi adalah menggunakan skema tanda tangan. Sistem kriptografi kunci publik dapat dimodifikasi menjadi suatu skema tanda tangan. Salah satunya adalah skema tanda tangan ElGamal, yaitu skema tanda tangan yang merupakan modifikasi dari sistem kriptografi kunci publik ElGamal. Sehingga tingkat keamanan skema tanda tangan ElGamal terletak pada kekuatan masalah logaritma. Sedangkan skema tanda tangan ElGamal pada Grup Eliptik atas Z_p merupakan skema tanda tangan ElGamal yang dikembangkan berdasarkan sistem kriptografi kurva eliptik atas Z_p.

Definisi

Suatu skema tanda tangan adalah suatu 5-tupel $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, dimana memenuhi kondisi berikut :

1. $\mathcal{P}$ adalah himpunan berhingga pesan,
2. $\mathcal{A}$ adalah himpunan berhingga tanda tangan,
3. $\mathcal{K}$ adalah himpunan berhingga kunci, disebut ruang kunci,
4. Untuk setiap $K \in \mathcal{K}$, terdapat fungsi tanda tangan $Sig_K \in \mathcal{S}$ dan fungsi verifikasi $Ver_K \in \mathcal{V}$. Setiap $Sig_K : \mathcal{P} \to \mathcal{A}$ dan $Ver_K : \mathcal{P} \times \mathcal{A} \to$ {benar, salah} merupakan fungsi sedemikian hingga untuk setiap pesan $x \in \mathcal{P}$ dan untuk setiap tanda tangan $y \subset \mathcal{A}$, persamaan berikut ini dipenuhi :

$$Ver_K(x,y) = \begin{cases} \text{benar, jika } y = sig_K(x) \\ \text{salah, jika } y \neq stg_K(x). \end{cases}$$

Berikut ini diberikan suatu skema tanda tangan yang menunjukkan bahwa masalah logaritma diskrit dapat diterapkan untuk membentuk suatu skema tanda tangan, seperti pada skema tanda tangan ElGamal. Skema ini merupakan modifikasi dari sistem kriptografi kunci publik ElGamal.

Sistem Kriptografi : Skema Tanda Tangan ElGamal pada Grup Eliptik atas Z_p. Diberikan bilangan prima (besar) p, diberikan kurva eliptik atas Z_p yaitu $E(Z_p)$, dan sebuah elemen pembangun atau generator $P \in E(Z_p)$. Sedemikian hingga $\langle P \rangle$ merupakan subgrup siklik dengan order prima (besar), yaitu $O(P) = q$.

Ditentukan $\mathcal{P} = \langle P \rangle$, $\mathcal{A} = \langle P \rangle \times \langle P \rangle$ dan $1 < k < q$-1. Didefinisikan

$$\mathcal{K} = \{(p, q, E(Z_p), k, Q) : Q = kP\}.$$

Nilai p, q, Q dipublikasikan, sedangkan nilai k dirahasiakan.

Untuk $\mathcal{K} = (p, q, k, Q)$ dan untuk suatu bilangan acak rahasia e dengan $1 \leq e \leq q$, didefinisikan

$$Sig_K(x,k) = (\gamma, \delta)$$

dengan

$$\gamma = x(eP) \bmod q$$

dan

$$\delta = (d + k\gamma)e^{-1} \pmod q$$

Untuk $\gamma, \delta \in \langle P \rangle \times \langle P \rangle$, didefinisikan

$$Ver_K(x,(\gamma,\delta)) = \text{benar} \Leftrightarrow x(v_1 P + v_2 Q) \bmod q = \gamma$$

Dengan

$$v_1 \equiv d\delta^{-1} \pmod q$$
$$v_2 \equiv \gamma\delta^{-1} \pmod q$$

Sama seperti pada sistem kriptografi kurva eliptik atas Z_p, tingkat keamanan dari skema tanda tanan ElGamal pada grup eliptik atas Z_p terletak pada kekuatan *Elliptic Curve Discrete Logarithm Problem* pada $\langle P \rangle$ dengan pembangun/ generator $P \in E(Z_p)$.

4. Penutup

Dari pembahasan diatas dapat disimpulkan bahwa *Elliptic Curve Discrete Logarithm Problem* dapat diterapkan pada skema tanda tangan ElGamal. Tingkat keamanan dari suatu skema tanda tangan ElGamal pada Grup Eliptik atas Z_p sebanding dengan tingkat kesulitan untuk menyelesaikan *Elliptic Curve Discrete Logarithm Problem.*

Pembahasan selanjutnya yang dapat dikaji mengenai metode untuk mencari bilangan prima yang besar, perhitungan order dari suatu elemen grup, dan metode untuk menghitung operasi perpangkatan modulo dan penjumlahan titik-titik kurva elliptik atas Z_p dengan cepat dan efisien.

Daftar Pustaka

Hoofstein, Phiper, and Silverman., 2008, *An Introduction to Mathematical Cryptography*, Springer, New York.

Hankerson, D., et.al., 2004, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York.

Stinson, D.R., 2006, *Cryptography Theory and Practice*, Chapman & Hall/CRC, Boca Raton, Florida.